Publication No. 2005/0088977), hereafter "Roch". (Office Action, page 3) The rejection is respectfully traversed.

CLAIM 1

Claim 1 recites:

1. A method for applying a quality of service to an encrypted packet comprising:

during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID;

examining an encrypted packet;

without decrypting the encrypted packet, mapping a second IKE ID from the packet, using the first IKE ID, to the identifier associated with the quality of service in a profile portion of the encrypted packet;

in response to mapping to the identifier associated with the quality of service, applying the associated quality of service to the encrypted packet.

The Office Action acknowledges that Buer does not disclose "receiving and storing an identifier associated with the quality of service," and acknowledges that Ben does not disclose the relation between QoS and IKE ID, but relies upon Roch (paragraphs 29-30 and 33-34) to show "**during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first IKE ID, without decrypting the encrypted packet, mapping a second IKE ID from the packet [...] to the identifier [...] and in response to mapping to the identifier associated with the quality of service, applying the associated quality of service to the encrypted packet.**" (Office Action, pages 3-4) This is incorrect.

One difference between claim 1 and Roch is that claim 1 uses of the IKE ID included in the header of the packet to identify QoS treatment for the packet, whereas Roch does not. According to claim 1, during the initial establishment of the IKE communication channel,

associations between particular QoS treatments and groups of IKE IDs are created, and once the IKE channel is established, the associations are queried to determine the QoS based on the IKE ID included in the header of the encrypted packet. In Roch, during the initial establishment of the communication channel for a particular subscriber, an existing association between the subscriber and QoS is queried, and once the communication channel is established, the queried QoS parameters for the particular subscriber are copied to the IKE headers. Thus, Roch does not use the IKE ID, and does not create an association at the same time as recited in claim 1.

In Roch, in order to obtain the QoS for the VPN tunnel, the VPN tunnel launches a policy request message to the policy server, which, in turn queries the policy database to obtain respective policy information concerning the subscriber. (Roch: paragraph 32) Upon receipt of the subscriber's policy information from the policy database, the policy server extracts and forwards the appropriate QoS parameters to the VPN ingress gateway. Based on the received QoS parameters, the VPN ingress gateway proceeds to negotiate a service association with the VPN egress gateway and set up the VPN tunnel. (Roch: paragraph 32) Once the VPN tunnel is set up, the VPN ingress gateway prepares the outer IP header, attaches it to the encrypted packet, and sends it to the egress VPN gateway. The outer IP header is prepared in a substantially conventional manner, with the exception that the value of the Differentiated Services Code Point (DSCP) field of the outer IP header is derived from the QoS parameters obtained from the policy server. (Roch: paragraph [33]) In particular, Roch may copy the QoS parameters obtained from the policy server to the next payload field (field values 14 through 127) of the ISAKMP/IKE policy update message.

According to Roch, the QoS treatment of tunnel traffic is determined by the contents of the DSCP field of the outer IP header, not based on the IKE ID field of the header, as claimed. In Roch, the QoS is determined from the value of the DSCP field determined by the policy server based on policy information respecting the subscriber stored in the policy database by querying the policy server, not identified using the IKE ID field of the header, as claimed. Roch's QoS are associated with the subscribers, not with the IKE IDs, as claimed.

Roch parses headers of the IKE protocol messages only to extract QoS treatment parameters stored in the "next payload field," not to extract the IKE ID to query associations between the IKE IDs and QoS treatments. Roch's QoS is indexed by the subscriber IDs, not by the IKE IDs. Therefore, Roch allow only one type of the QoS treatment per subscriber. To assign a different QoS treatment, Roch dismantles the VPN tunnel and alters its policy database. (Roch: paragraph 30) Roch does not allow changing the QoS treatment at the IPSec protocol level.

In fact, Roch teaches away from negotiating the QoS treatment as a part of the security association at the IPSec protocol level. In paragraph 29, Roch states "Because the IPSec protocol does not incorporates negotiation of the QoS treatment as part of the security associate established during tunnel setup by the VPN gateways, in the event of that a subscriber wishes to alter the QoS treatment of traffic within the tunnel, it is not possible to renegotiate the security association (with QoS changes) between the VPN gateways.

In sharp contrast to Buer, Ben and Roch, claim 1 recites that "**during initial establishment of a secure control channel, receiving and storing an identifier associated with the quality of service in association with a first IKE ID, without decrypting the encrypted packet, mapping a second IKE ID from the packet [...] to the identifier [...] and in response to mapping to the identifier associated with the quality of service, applying the associated quality of service to the encrypted packet.**" As described in applicants' specification (paragraphs 40-41 and 60), using the IKE identifiers to identify QoS treatments has a number of benefits. For example, instead of sending the same QoS and IKE data in each data packet for each user within a class of users, storing associations between QoS identifiers and IKE identifiers for classes of users allows equal application of the same QoS to each user within the class. Further, indexing a set of IKE functions and QoS functions, using just one identifier sent in the clear in the packet, allows execution of QoS on the packet before a time-consuming decryption of the packet even begins.

Storing associations between QoS identifiers and IKE identifiers during an initial establishment of the secure control channel is also beneficial in VPN environments, as described in applicants' specification (paragraph 60). For example, in a VPN environment, where customers use overlapping address spaces within the internal networks, IPsec would cause encrypting of the payload of an original packet, and thus obscure the original packet header containing QoS instructions. Obscuring the original packet header makes the QoS instructions unreadable, and thus, makes it impossible to apply QoS in accordance with the original packets contents until the packet is actually decrypted.

However, if, "**during initial establishment of a secure control channel, [...] an identifier associated with the quality of service in association with a first Internet Key Exchange (IKE) ID is received and stored,**" as in claim 1, the association between the IKE identifiers and the QoS identifiers is created, and can be used to retrieve the QoS identifiers indirectly using a mapping approach. This provides an efficient service mechanism, wherein QoS functions can be identified using just IKE identifiers. Subsequently, QoS functions can be successfully applied to IPsec protected (encrypted) packets. (Specification, paragraph 60) This is not taught or suggested in Buer, Ben and Roch, individually or in combination.

Therefore, at least one element of claim 1 is not disclosed, taught or suggested by the combined prior art. Thus, it is respectfully submitted that Buer, Ben and Roch, individually and in combination, fail to disclose the complete subject matter recited in claim 1.

Reconsideration and withdrawal of the rejection is respectfully requested.

CLAIMS 11, 14, 27 AND 37

Claims 11, 14, 27 and 37 recite features similar to those in claim 1. Therefore, applicants believe that claims 11, 14, 27 and 27 are patentable over Buer and Ben for the same reasons discussed for claim 1.

B. CLAIMS -- 35 U.S.C. § 103(a): BUER, BEN AND PIPER

Claims 4, 8, 17, 21, 30, 40, 44 and 48 are rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable over Buer and Ben and in view of Piper's "The Internet IP Security

Domain of Interpretation for ISAKMP" (November, 1998). (Office Action, page 7) The rejection is respectfully traversed.

Claims 4 and 8 depend directly or indirectly from claim 1, claims 17 and 21 depend directly or indirectly from claims 14, claim 30 depends indirectly from claim 27, and claims 40, 44 and 48 depend directly or indirectly from claim 37. As discussed above, Buer and Ben, individually and in combination, fail to teach and suggest independent claims 1, 14, 27 and 37.

Further, Piper fails to cure the deficiencies of Buer and Ben with respect to independent claims 1, 14, 27 and 37. Therefore, because Buer, Ben and Piper, individually and in combination, fail to provide all subject matter recited in claims 1, 8, 14, 27 and 37, and due to claim dependency, claims 4, 8, 17, 21, 30, 40, 44 and 48 are patentable over Buer in view of Ben and in further view of Piper.

Reconsideration and withdrawal of the rejection are respectfully requested.

C. CLAIMS -- 35 U.S.C. § 103(a): BUER, BEN AND VALENCI

Claims 9-10, 12, 22-23, 45-46 and 49-50 are rejected under 35 U.S.C. § 103(a) as being allegedly anticipated by Buer and Ben and in view of Valenci et al. (U.S. Patent Publication No. 2003/0005279), hereafter "Valenci." (Office Action, page 9) The rejection is respectfully traversed.

Claims 9-10 and 12 depend directly or indirectly from claim 1, claims 22-23 depend directly or indirectly from claim 14, and claims 45-46 and 49-50 depend directly or indirectly from claim 37. As discussed above, Buer and Ben, individually and in combination, fail to teach and suggest independent claims 1, 14, 27 and 37.

Further, Valenci fails to cure the deficiencies of Buer and Ben with respect to independent claims 1, 14, 27 and 37. Therefore, because Buer, Ben and Valenci, individually and in combination, fail to provide all subject matter recited in claims 1, 14, 27 and 37, and due to claim dependency, claims 9-10, 12, 22-23, 45-46 and 49-50 are patentable over Buer in view of Ben and in further view of Valenci.

Reconsideration and withdrawal of the rejection are respectfully requested.